CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

1. I, Scott Bauer, am currently employed as a Special Agent with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI), and have been so employed since March of 2012. I am currently assigned to HSI Grand Rapids, MI. During my employment with HSI, I have received training and conducted investigations into a wide variety of federal criminal laws, to include fraud and intellectual property violations. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. Prior to employment with HSI, I was employed as a Special Agent with United States Department of the Interior (DOI), Office of the Inspector General (OIG), for approximately four years, where I investigated fraud, waste and abuse related to the Department of Interior. Prior to that, I was a Police Officer with the City of Casselberry, Florida, for approximately two years and eight months.

INTRODUCTION AND PURPOSE OF THE WARRANT

3. I make this affidavit in support of an application for a search warrant to search **3893 Werner Street, Norton Shores, MI 49444,** further described in Attachement A, for evidence, contrabands, fruits, and instrumentalities of crimes in violation of 18 U.S.C. §1341 (frauds and swindles) and 18 U.S.C. §1343 (fraud by wire, radio, or television).

4. I am familiar with the information contained in this continuation based upon the investigation I have conducted and based on information provided to me by

other law enforcement officers.

5. The facts in this continuation come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this continuation is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

FACTUAL BACKGROUND OF INVESTIGATION

6. In December of 2020, I spoke with Mary and Andy Frisinger via telephone. The Frisingers paid Bryan KENNERT approximately $43,354 over the course of approximately six months in 2019 for what they believed were authentic vintage baseball card packs. The packs were ultimately determined to be fraudulent (this is further detailed in a subsequent paragraph). Additionally, the Frisingers spent approximately $1,021.75 in authentication fees.

7. The Frisingers became acquainted with KENNERT while looking for baseball cards at the Anything and Everything Antique Mall in Muskegon, MI. Andy Frisinger noticed an unoccupied booth with baseball cards for sale. As the booth was unoccupied, Andy Frisinger left a message with Anything and Everything staff inquiring about the items. Customers are unable to communicate directly with sellers if the sellers are not present.

8. Ultimately, the victims met with KENNERT on numerous occasions throughout 2019 and made several purchases of vintage baseball cards from KENNERT.

These purchases were arranged via cellular telephone and occurred in the parking lot of the Anything and Everything Antique Mall. The purchases were facilitated via debit and credit card transactions made payable to Anything and Everything Antique Mall. During these purchases, Andy Frisinger recalled KENNERT driving a red Chevrolet Equinox.

9. The Frisingers described the packs they purchased as rare and had not been observed for sale for approximately 11 years. Upon receipt of some of these packs, Andy Frisinger noticed the packs appeared to be glued back together, and a Michael Jordan rookie card discovered in one of the packs was too large to fit into a standard protective case.

10. In February of 2020, the victims met with Steve Hart from The Baseball Card Exchange to examine the cards for authenticity. Hart and the Baseball Card Exchange provide sports memorabilia authentication services and according to their website, www.bbcexchange.com, "Baseball Card Exchange is recognized as the industry leader in unopened vintage sports cards, and Steve Hart has become the most respected and trusted authenticator of unopened wax product." Hart had been studying unopened packs for 30 years and was employed by Professional Sports Authenticator (PSA), the world's largest authenticator for sports cards and sports related items. Hart had served as an expert witness at trial and had been requested to dispute hundreds of eBay/PayPal/Auction houses cases related to tampered items.

11. The following items purchased by the Frisingers from KENNERT were reviewed by Hart and detailed in a written finding provided to the Frisingers, who in

turn provided it to SA Bauer in January of 2021:

a. 1952 Topps baseball

b. (2) 1933 Goudey Sports Kings

c. 1933 Goudey baseball

d. 1936 Goudey baseball

e. (2) 1954 Bowman football

f. 1986/1987 Fleer basketball (with a Michael Jordan rookie card on the top of the pack)

g. (2) 1968 Topps Doubleheaders

h. 1955 Topps Doubleheaders

i. (2) 1963 Topps baseball 5 cent

j. (6) 1968 Topps baseball

k. (3) 1969 Topps baseball

l. (2) 1962 Topps baseball

m. (4) 1965 Topps baseball

n. 1970 Topps baseball

o. (2) 1979 Topps baseball

p. (6) 1967 Topps baseball

q. 1971 Topps baseball

r. 1972 Topps baseball

s. 1973 Topps baseball

t. (4) 1966 Topps baseball

u. (5) 1968 Topps football

v. (2) 1965 Topps football

w. 1961 Topps football

x. 1966 Topps football

y. 1967 Topps football

z. (11) 1975 Topps football

aa. (2) 1971 Topps football

bb. (2) 1970 Topps football

cc. 1974 Topps football

dd. 1975 Topps football

12. Upon inspection of the items, Hart determined the packs had been, "Tampered with and resealed." According to Hart, the resealing was done poorly and consistently, leading him to conclude that it was done by the same person. Hart requested one of his employees review the items for a second opinion. This employee came to the same conclusion.

13. If authentic, Hart stated the value would be in the $200,000 range, however these packs were only a small fraction of that. Hart explained to the Frisingers the items were "100% complete garbage" and were "Nearly worthless."

14. According to Andy Frisinger, KENNERT stated he previously owned two sports card shops (in Ludington and Muskegon) in the 1980s, but KENNERT became burnt out and placed all of his products into storage. KENNERT told Andy Frisinger he had several cases of cards at his home, which he hadn't reviewed yet and which he

received from his father. KENNERT also stored cards in a warehouse, which he shared with another unknown individual. KENNERT stated he did not like card grading and was no longer collecting cards. Additionally, KENNERT stated he sold other types of antiquities, which he received after his parents' death.

15. A review of KENNERT's criminal history revealed previous federal arrests and convictions for fraud and trafficking in counterfeit goods between 1987 and 1996. In approximately 1992, and in a previous U.S. Customs Detroit case, KENNERT plead guilty to importing counterfeit baseball cards from Hong Kong and selling them as legitimate.

16. In April of 2021, SA Bauer received information from FBI Grand Rapids regarding a 2014 investigation into KENNERT. This investigation centered around KENNERT and a box of resealed baseball cards, specifically a box of 1969 Topps baseball cards. According to FBI documents, KENNERT attempted to have the resealed cards sold at auction. Ultimately the cards were discovered to be fraudulent before they were sold.

17. In 2014, the FBI interviewed KENNERT who admitted the packs were fraudulent. KENNERT told the FBI during his time in prison he acquired the skills to obtain individual's private information, to include Social Security Numbers and credit card numbers. KENNERT also stated he utilized several PayPal and eBay accounts that could not be traced back to him and learned how to circumvent PayPal's security scrutiny.

18. KENNERT told the FBI he worked in China in 2007 and 2008 and during that time made contacts with various counterfeiters of sports cards, coins, and US

currency. KENNERT provided these individuals with advice on quality and strategies. KENNERT stated he smuggled suitcase loads of currency from China to Hong Kong.

19. KENNERT told the FBI his business model was dealing with graded sports cards and he utilized shell companies, filed under false identities, to sell the cards. KENNERT told the FBI he made enough money in China that he did not need to work upon his return to the United States.

20. KENNERT stated he destroyed approximately one dozen 800 count boxes of raw counterfeit cards at his house prior to meeting with the FBI.

21. On June 18, 2021, the following communication occurred between victim Andy Frisinger (AF) and KENNERT (all grammatical errors are from the original and only relevant portions of the communication are detailed below):

- AF: BRIANnnnn. Whats up man, i was driving by anything and everything a couple days ago and thought of you. Wondering if your e doing ok. Weve been through a shit show last year. This is your baseball card friend andy in case im not logged in your phone. Also wanted to know if you found anymore packs? Just checking.
- KENNERT: I texted you about a year ago twice and didn't get an answer I thought something bad happened thank goodness, maybe we missed each other I sold everything there but i still have a bunch of packs, of course it was a bad last year

22. Additionally, KENNERT stated he planned to have an estate sale in August of 2021 where he planned to sell "a lot of my cards and memorabilia" and cited "my 1945 tigers auto tigers photo 1968 worlds series pennant 1984 pennant" and later stated in part,

"I was going to sell many of my packs" referring to the estate sale. KENNERT stated, "I can sell whatever I want before the 23 of July that's when they take over what I leave in the house then they get it ready for the august estate sale on the 19 20 and 21 of august 3893 Werner in muskegon if you want to know."

23. Through the use of law enforcement databases, SA Bauer learned KENNERT's home address was 3893 Werner Street, Norton Shores, MI 49444 (the same address provided to the FBI in 2014). A review of Norton Shores public records revealed this residence was owned by KENNERT. A red colored Chevrolet Equinox bearing Michigan license plate CDP573 was registered to KENERT at 3893 Werner Street, Norton Shores, MI 49444.

24. In June of 2021, and pursuant to a court order, HSI Grand Rapids placed a GPS tracker on the previously mentioned Equinox. As of June 29, 2021, the vehicle was located at 3893 Werner Street in Norton Shores.

SPECIFICS OF SEIZING AND SEARCHING COMPUTER SYSTEMS

25. Computers and Internet-capable devices such as tablets and cellular telephones facilitate communication regarding a counterfeit baseball cards or sports memorabilia, specifically through the use of online auction and payment sites like those mentioned by KENNERT.

26. Storage capacity of computers and portable storage media, such as cellular telephones and USB or thumb drives, has grown tremendously in recent years. These devices can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the

size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places, such as in vehicles or outbuildings associated with a residence. An individual can now easily carry on his or her person, or store in any number of places, storage media that contains thousands of files, including images, video files, and full-length movie files.

27. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer or cellular phone user's Internet activities generally leave traces in the device's web cache and Internet history files.

28. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file often does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants

of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

29. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and device habits.

30. Searches and seizures of evidence from computers, computer devices, and cellular phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Electronic devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes

the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching electronic devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to retrieve data fully from an electronic device, the analyst needs all storage devices as well as the central processing unit (CPU). In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

32. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer or electronic device at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms

of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

33. The time required for a complete, safe, and secure forensic examination of the computer and electronic devices is uncertain. The Government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

34. Items determined on-scene not to contain items listed in Attachment B will be left. The remaining items will be seized and searched for further review or forensic examination and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Attachment B.

35. Retention of any devices would be warranted, if any evidence of communications indicating an intent to violate 18 U.S.C. § 1341 or 18 U.S.C. § 1343 is

found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. § 2428.

REQUEST FOR BIOMETRIC UNLOCK

36. Based on my knowledge and experience, I know that certain cellular telephones, including Apple iPhones, and some personal computers may be locked and/or unlocked by personal identification numbers (PIN), gestures or motions, and/or with biometric features, such as thumb and fingerprint recognition (collectively, "fingerprint ID") and/or facial recognition ("facial ID").

37. If a user enables the fingerprint ID unlock feature on a device, he or she can register several fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's sensor, which typically is found on the front of the device. In my training and experience, users of devices that offer fingerprint ID or facial ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

38. In some circumstances, a fingerprint or face cannot be used to unlock a device, and a passcode or password must be used instead. Depending on the configuration of the security settings on the phone, the opportunity to unlock the device via fingerprint ID or facial ID exists only for a short time. Fingerprint ID and facial ID

also may not unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) several unsuccessful attempts to unlock the device are made.

39. The passcode or password that would unlock the device(s) found during the search is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) or present the face of the user(s) of the device(s) found during the search to the device's fingerprint ID or facial ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via fingerprint ID or facial ID is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

40. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s), this will result in the device requiring the entry of a password or passcode before it can be unlocked.

41. Based on the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of BRYAN KENNERT to the fingerprint ID sensor or to present his face to the facial ID sensor of any seized device(s) to attempt to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

42. Based on the above information, I respectfully submit that there is probable

cause to believe that evidence, fruits, and instrumentalities of criminal offenses in violation of 18 U.S.C. §§ 1341 and 1343 may be found at 3893 Werner Street, Norton Shores, MI 49444

43. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.